CZU 343.534:343.144.5 DOI 10.5281/zenodo.8318129

APLICAREA CUNOȘTINȚELOR SPECIALE PENTRU DETECTAREA COMPORTAMENTULUI SIMULAT LA CERCETAREA SPIONAJULUI ECONOMIC ȘI INDUSTRIAL

Iurie ODAGIU,
doctor în drept, conferențiar universitar
Andrei LUNGU,
doctorand,
master în drept, master în psihologie

Spionajul economic și industrial reprezintă, astăzi, o problemă extrem de gravă, pentru multe țări și companii, pe măsură ce tehnologiile au continuat să se dezvolte și să devină tot mai sofisticate.

Investițiile importante realizate de multe companii și corporații pentru dezvoltarea proprietății intelectuale sunt ținte profitabile pentru cei care doresc să se angajeze în acte de spionaj.

În acest articol ne propunem o definire a riscurilor legate de spionajul industrial și cel corporativ. Vom analiza formele ce le îmbracă acțiunile ilegale ale angajaților corporațiilor mari în vederea obținerii informațiilor restricționate și să propunem unele metode de prevenire și depistate a acestora la etapa angajării.

Vom face referire la aspecte legate de analiza comportamentală a persoanelor și vom veni cu recomandări în acest sens.

Cuvinte-cheie: detectarea minciunii, securitate cibernetică, comportament simulat, spionaj economic, interviu, analiză comportamentală, poligraf.

Introducere. Pentru marea majoritate a persoanelor cu funcție de conducere și manageri, aspectele legate de securitatea întreprinderilor comerciale și necomerciale, mari și mici, industriale sau din sfera serviciilor nu intră în domeniul lor de activitate. Securizarea organizației/întreprinderii este cel mai adesea responsabilitatea serviciului de securitate.

Din păcate, mulți conducători consideră o protecție calitativă doar cea care se referă la securitatea de amenințări și riscuri împotriva agresiunilor de ordin fizic, neținând cont de un

APPLYING SPECIAL KNOWLEDGE OF SIMULATED BEHAVIOR DETECTION TO ECONOMIC AND INDUSTRIAL ESPIONAGE RESEARCH

Iurie ODAGIU,
PhD, associate professor
Andrei LUNGU,
PhD student,
master in law, master in psychology

Economic and industrial espionage represents, today, an extremely serious problem for many countries and companies, as technologies have continued to develop and become increasingly sophisticated.

The heavy investments made by many companies and corporations to develop intellectual property are prosperous targets for those who wish to engage in acts of espionage.

In this article, we propose a definition of the risks related to industrial and corporate espionage. We will analyze the forms that the illegal actions of employees of large corporations take in order to obtain restricted information and propose some methods of their prevention and detection at the employment stage.

We will refer to aspects related to the behavioral analysis of people and come up with recommendations in this regard.

Keywords: lie detection, cyber security, simulated behavior, economic espionage, interview, behavioral analysis, polygraph.

Introduction. For the vast majority of executives and managers, issues related to the security of commercial and non-commercial, large and small, industrial or service enterprises do not fall within their scope of activity. Securing the organization/enterprise is most often the responsibility of the security service.

Unfortunately, many managers consider a qualitative protection only that which refers to the security of threats and risks against physical aggressions, not taking into account a growing phenomenon, which is known as "in-

fenomen în plină dezvoltare, care este cunoscut sub denumirea de „infracţiuni de proprietate intelectuală".

Acest flagel, cu regret, nu a suscitat un interes deosebit din partea mediului academic şi la ora actuală nu face parte din domeniul de cercetare în Republica Moldova sub aspect criminalistic. Varietatea problemelor ce ar trebui să fie analizate în detaliu se referă la „spionajul economic şi comercial", „spionajul industrial", „spionajul corporativ", „spionajul cibernetic" etc.

În condiţiile zilei de astăzi, când există o practica răspândită ce se referă la concurenţa neloială, o astfel de atitudine neglijentă din partea managerilor întreprinderilor de a proteja companiile de riscurile şi ameninţările reprezentate de infracţionalitatea în domeniul proprietăţii intelectuale ar putea duce la pierderi considerabile sau chiar la faliment.

Scopul studiului. Autorii îşi propun să facă o analiză doctrinară a fenomenului ce se referă la securitatea companiilor privind riscurile atacurilor asupra proprietăţii intelectuale şi procedeele de combatere a acestora. Urmează definirea acţiunilor de spionaj comercial şi elaborarea recomandărilor pentru prevenirea şi profilaxia acestora.

Acest articol face referire la securizarea agenţilor economici împotriva riscurilor şi ameninţărilor ce ar putea veni din partea personalului angajat, ca urmare a erorilor de evaluare a acestora. Problematica acestui studiu are relevanţă atât în structurile statale, cât şi în sectorul privat.

Autorii vor aborda aspecte legate de analiza comportamentală a angajaţilor, detecţia neinstrumentală şi instrumentală a minciunii în cadrul interviului corporativ, posibilitatea aplicării poligrafului la nivelul de evaluare a loialităţii personalului, precum şi la stabilirea intenţiilor de spionaj comercial. Acest subiect face parte din zona ştiinţelor interdisciplinare cum ar fi: criminalistica, psihologia, managementul, criminologia şi sociologia.

Metode şi materiale aplicate. Cercetarea va fi realizată prin valorificarea metodei de cercetare specifice teoriei şi doctrinei juridice, cum ar fi: metoda logică, metoda analizei comparative, analiza sistemică, descrierea, deducţia, metoda istorică. Materialele utilizate în vederea realizării studiului: publicaţii ale

tellectual property crimes".

This scourge, regrettably, did not arouse special interest from the academic environment and is currently not part of the field of research in the Republic of Moldova from a forensic aspect. The variety of issues that should be analyzed in detail refer to "economic and commercial espionage", "industrial espionage", "corporate espionage", "cyber espionage", etc.

In today's conditions, when there is a widespread practice of unfair competition, such a negligent attitude on the part of business managers to protect companies from the risks and threats posed by intellectual property crime could lead to considerable losses or even to bankruptcy.

The purpose of the study. The authors propose to do a doctrinal analysis of the phenomenon that refers to the security of companies regarding the risks of attacks on intellectual property and methods of combating them.

Next comes the definition of commercial espionage actions and the development of recommendations for their prevention and prophylaxis.

This article refers to the securing of economic agents against the risks and threats that could come from the employed personnel, as a result, of their evaluation errors.

The issue of this study has relevance both in state structures and in the private sector.

The authors will address issues related to the behavioral analysis of employees, the non-instrumental and instrumental detection of lies in the corporate interview, the possibility of applying the polygraph at the level of evaluating staff loyalty, as well as establishing commercial espionage intentions.

This subject is part of the area of interdisciplinary sciences such as: forensics, psychology, management, criminology and sociology.

Applied methods and materials. The research will be carried out by capitalizing on the research method specific to legal theory and doctrine, such as: logical method, comparative analysis method, systemic analysis, description, deduction, historical method. The materials used to carry out the study are the publications of researchers in the field, analytical materials of practitioners, as well as the relevant legislation. In addition, the scientific

cercetătorilor din domeniu, materiale analitice ale practicienilor, legislaţia relevantă. De asemenea, baza ştiinţifică a cercetării o constituie diverse studii cuprinse în culegeri de materiale ale conferinţelor, articole ştiinţifice, comentarii aplicative etc.

Rezultate obţinute şi discuţii. Zilnic, în lumea companiilor mari ne confruntăm cu acte ilicite, fraude şi înşelătorii. Atunci când concurenţa acerbă dintre agenţii economici, lăcomia proprietarilor acestora şi goana după bani depăşeşte anumite norme etico-morale, pot lua naştere activităţi frauduloase.

Competiţia şi concurenţa în esenţa sa nu este un lucru rău, deoarece motivează evoluţia. Fiind concurenţă pe piaţă, fiecare actor economic doreşte să exceleze şi să fie înaintea celorlalţi în aceeaşi activitate. Atunci când se respectă normele legale, activitatea comercială este justificată, dar există situaţii care alunecă în zona activităţilor frauduloase. Ne referim la spionajul corporativ sau industrial, care reprezintă o problemă gravă pentru multe companii.

Într-o altă ordine de idei, cei care doresc să supravieţuiască în lumea afacerilor trebuie să fie precauţi şi puternici şi să-şi securizeze businessul sub toate aspectele.

Activitatea cea mai răspândita în lumea afacerilor este spionajul corporativ. În acest context, vom opera cu definiţia spionajul economic ca fiind acţiunea de a fura secretele comerciale ale companiei cu intenţie sau ştiinţă, propusă de Benjamin C. Glassman, Matt Wagner şi Colin R. Jennings [1].

Definiţia profesorului Robert E. Wagner - assistant Professor of Law City University of New York (CUNY), Baruch College Zicklin School of Business, Department of Law One Bernard Baruch Way New York, NY10010, rămâne a fi fundamentală: „Spionajul economic se referă la direcţionarea sau achiziţionarea secretelor comerciale, sustrase de la companii naţionale sau entităţi guvernamentale, în beneficiul unui stat străin" şi „Spionajul industrial se referă la acelaşi lucru, ca şi spionajul economic, cu excepţia faptului că de acesta beneficiază, mai degrabă, o entitate privată decât un guvern străin" [2].

Reieşind din definiţiile de mai sus, deducem că chiar dacă aceste două tipuri de activităţi au scopuri diferite, acţiunile întreprinse sunt similare şi în acest context distin-

basis of the research is constituted by various studies contained in collections of conference materials, scientific articles, application comments, etc.

Results obtained and discussion. Every day in the world of large companies we are faced with illegal acts, fraud and scams. When the fierce competition between economic agents, the greed of their owners and the rush for money exceeds certain ethical and moral norms, fraudulent activities can arise.

Competition and contention in its essence is not a bad thing because it motivates evolution. Being competitors in the market, everyone wants to excel and be ahead of others in the same activity. When the legal norms are respected, the commercial activity is justified, but there are situations that slip into the area of fraudulent activities.

We are referring to corporate or industrial espionage, which is a serious problem for many companies.

On another note, those who want to survive in the business world for a long time must be cautious and strong and secure their businesses in all aspects.

The most widespread activity in the business world is corporate espionage.

In this context, we will operate with the definition of economic espionage as the act of stealing company trade secrets with intent or knowledge, proposed by Benjamin C. Glassman, Matt Wagner and Colin R. Jennings[1].

The definition of Professor Robert E. Wagner - assistant Professor of Law City University of New York (CUNY), Baruch College Zicklin School of Business, Department of Law One Bernard Baruch Way New York, NY10010, remains fundamental: "Economic espionage refers to directing or acquiring trade secrets, stolen from national companies or government entities, for the benefit of a foreign state" and "Industrial espionage refers to the same thing as economic espionage, except that it benefits, rather, an entity private, than a foreign government" [2].

Based on the above definitions, we deduce that even if these two types of activities have different goals, the actions undertaken are similar and in this context, we distinguish two basic key elements:

gem două elemente cheie de bază:

➢ Factorul uman – prin natura lui este un element forte sau veriga slabă în prevenirea activităţilor de spionaj;

➢ Factorul tehnic – explorează vulnerabilităţile IT şi securitatea cibernetică.

Un exemplu de spionaj economic realizat prin implicarea factorului uman este situaţia anului 1965, când România trecea într-o nouă eră economică şi politică. N. Ceauşescu şi-a propus să transforme ţara în unul din cele mai mari şi importante centre industriale din estul Europei.

Urmare a unui ordin, dat generalului de securitate Ion Mihai Pacepa în vederea obţinerii unei performanţe pentru producerea autoturismului autohton, a fost demarată o operaţiune secretă de dobândire a tehnologiei de fabricaţie a acestuia, care să devină mândria ţării.

Soluţia a venit de la francezi – aşa a ajuns Renault 10 să se numească Dacia 1100, iar industria românească să ia avânt. Dacia 1100 a fost un succes al spionajului economic şi a devenit un instrument al guvernării de atunci, de care era responsabilă Direcţia de Informaţie Externă a României.

În câţiva ani au fost formaţi sute de agenţi secreţi: ingineri, chimişti sau fizicieni infiltraţi în companii străine pentru a prelua informaţii, schiţe şi proiecte în vederea realizării ulterioare a acestora în România.

Un caz de spionaj industrial este cel în favoarea companiei Pepsi, realizat de Joya Williams, în vârstă de 42 de ani, care a fost condamnată la opt ani de privaţiune de libertate, iar complicele său, Ibrahim Dimson, a primit o sentinţă de cinci ani. Amândoi au fost amendaţi cu 40.000 de dolari. Aceştia au fost acuzaţi de tentativa vinderii documentelor secrete ale companiei Coca Cola concurentului său de bază pe piaţa americană – Pepsi, contra sumei de 1,5 milioane de dolari [3].

Considerăm că securizarea personalului angajat este un element extrem de important în contracararea spionajului economic şi industrial. În acest context ne referim şi la neadmiterea angajării persoanelor ce au intenţii ce presupun activităţi de furt intelectual.

Angajaţii unei companii sunt componenta principală care contribuie la bunăstarea acesteia; or, dacă aceasta din urmă nu este ad-

➢ The human factor - by its nature it is a strong element or weak link in the prevention of espionage activities;

➢ The technical factor – explores IT vulnerabilities and cyber security.

An example of economic espionage achieved through the involvement of the human factor is the situation in 1965, when Romania was entering a new economic and political era. N. Ceauşescu set out to transform the country into one of the largest and most important industrial centers in Eastern Europe.

Following an order given to security general Ion Mihai Pacepa in order to achieve a performance in the production of domestic cars, a secret operation was started to acquire the manufacturing technology for it, which would become the pride of the country.

The solution came from the French people – that is how the Reno 10 came to be called the Dacia 1100, and the Romanian industry took off.

The Dacia 1100 was a success of economic espionage and became a tool of the government at the time, for which the Department of Foreign Information of Romania was responsible.

In a few years, hundreds of secret agents were formed: engineers, chemists or physicists infiltrated into foreign companies to take over information, sketches and projects with a view to their subsequent realization in Romania.

A case of industrial espionage is the one in favor of the Pepsi company, made by 42-year-old Joya Williams, who was sentenced to eight years in prison, and her accomplice, Ibrahim Dimson, received a five-year sentence. Both were fined $40,000.

They were accused of trying to sell the secret documents of the Coca Cola company, its main competitor on the American market – Pepsi, for the sum of 1.5 million dollars [3].

We believe that securing the employed personnel is an extremely important element in countering economic and industrial espionage. In this context, we also refer to the non-admission of employment of people who have intentions that involve intellectual theft activities.

The employees of a company are the main component that contributes to their well-being, or if it is not managed correctly, it can

ministrată corect, există ameninţarea creării unor riscuri şi pericole comerciale.

Se impune totuşi o delimitare a noţiunilor de risc şi de pericol comercial.

Considerăm că în categoria riscurilor de personal se încadrează înţelesul de management defectuos – atunci când administratorul în mod intenţionat sau din neglijenţă admite la serviciu un angajat ce nu îşi îndeplineşte calitativ îndatoririle funcţionale.

Pericolul comercial apare atunci când admitem la exercitarea funcţiei persoane care au intenţii de furt intelectual, sabotaj, activitate de fraudă corporativă, acte coruptibile, etc.

Se consideră că dauna adusă intenţionat de către angajat este mai nocivă şi periculoasă decât o simplă neglijenţă în serviciu [4].

În această ordine de idei, se impune o atenţie sporită şi o bună cunoaştere a tehnicilor de „profiling" corporativ în cadrul interviului la angajarea persoanei, precum şi o monitorizare a acesteia pe perioada de probă.

În viziunea noastră, „profiling"-ul corporativ este un set de metode şi tehnici, dezvoltate pentru alcătuirea unui portret psiho-emoţional al candidatului cu scopul evaluării ulterioare a acestuia pentru a determina comportamentul său. Utilizarea acestor tehnici contribuie la: prognozarea riscurilor de personal şi manageriale, determinarea loialităţii faţă de regulile şi reglementările stabilite de companie, detectarea minciunii pe cale neinstrumentală, stabilirea principalelor modele comportamentale, sociale, economice şi financiare.

Instrumentele de profilare vă vor permite să interpretaţi în mod obiectiv mesajele verbale şi non-verbale ale candidatului, să evaluaţi aspectul exterior al acestuia, fapt care va face posibilă o prezicere a comportamentului acestuia într-o situaţie sau circumstanţă de interes pentru angajator.

Structura fiinţei umane este de aşa natură, încât minciuna ne este improprie. Atunci când intenţionăm să denaturăm adevărul, facem un anume efort psiho-emoţional şi prin urmare simţim un fel de disconfort emoţional.

Profilarea se bazează pe determinarea comportamentului de bază al persoanei, atunci când nu există necesitatea de a spune neadevăr şi o ulterioară analiză comportamentală, ca reacţie la anumiţi stimuli.

create commercial risks and dangers.

However, a delimitation of the notion of commercial danger risks is required.

We believe that the category of personnel risks includes the meaning of faulty management - when the administrator intentionally or negligently admits to the knowledge of an employee who does not fulfill his functional duties qualitatively.

Commercial danger appears in cases when we admit to the exercise of the function persons who have intentions of intellectual theft, sabotage, corporate fraud activity, corrupt acts, etc.

It is considered, that the damage caused intentionally by the employee is more harmful and dangerous than a simple negligence in the service [4].

In this vein, greater attention and a good knowledge of "corporate profiling" techniques are required during the interview when hiring the person, as well as monitoring during the probationary period.

In our view, corporate "profiling" is a set of methods and techniques, developed to create a psycho-emotional portrait of the candidate for the purpose of his subsequent evaluation in order to determine his behavior. The use of these techniques contributes to forecasting personnel and managerial risks, determining loyalty to the rules and regulations established by the company, detecting lies by non-instrumental means, establishing the main social, economic and financial behavioral models.

Profiling tools will allow you to objectively interpret the candidate's verbal and non-verbal messages, evaluate his external appearance, which will make it possible to predict his behavior in a situation or circumstance of interest to the employer.

The structure of the human being is such that lying is inappropriate for us. When we intend to distort the truth, we make a certain psycho-emotional effort and therefore re-experience a kind of emotional discomfort.

Profiling is based on determining the basic behavior of people, when there is no need to tell untruths, and subsequent behavioral analysis, in reaction to certain stimuli.

Most of us will avoid telling lies, because this puts us in the discomfort zone and will

Majoritatea din noi vom evita a spune minciuni, pentru că acest lucru ne aduce în zona de disconfort şi prin urmare va da naştere unor reacţii fiziologice, care pot fi interpretate. Multe reacţii fiziologice, care însoţesc comportamentul simulat, se formează în zona sistemului nervos vegetativ şi nu pot fi controlate prin voinţă.

În consecinţă, un „profiler" experimentat acţionează în felul următor: el studiază comportamentul unei persoane într-o situaţie în care aceasta nu este impusă să mintă. De exemplu, poartă o discuţie abstractă şi relaxantă cu intervievatul, după care urmează etapa când sunt utilizaţi stimulii. Stimulii de obicei sunt auditivi, sub forma întrebărilor, dar pot fi folosiţi şi stimuli vizuali sau sonori.

Recomandăm intervievatorilor să se inspire din procedeele tactice folosite la audiere, cum ar fi: folosirea probelor de vinovăţie sau tactica întâlnirilor surpriză [5].

Se consideră extrem de valoroşi intervievatorii cu o experienţă în activitatea de ofiţer de urmărire penală, procuratură, activitate specială de investigaţii – oameni care în virtutea profesiei lor au desfăşurat multe activităţi specifice, similare interviurilor.

Pe timpul interviului vor fi atent analizaţi indicii non-verbali şi para-verbali ai intervievatului. Ponderea transmiterii informaţiei de către o persoană se exprimă în următoarea proporţie:

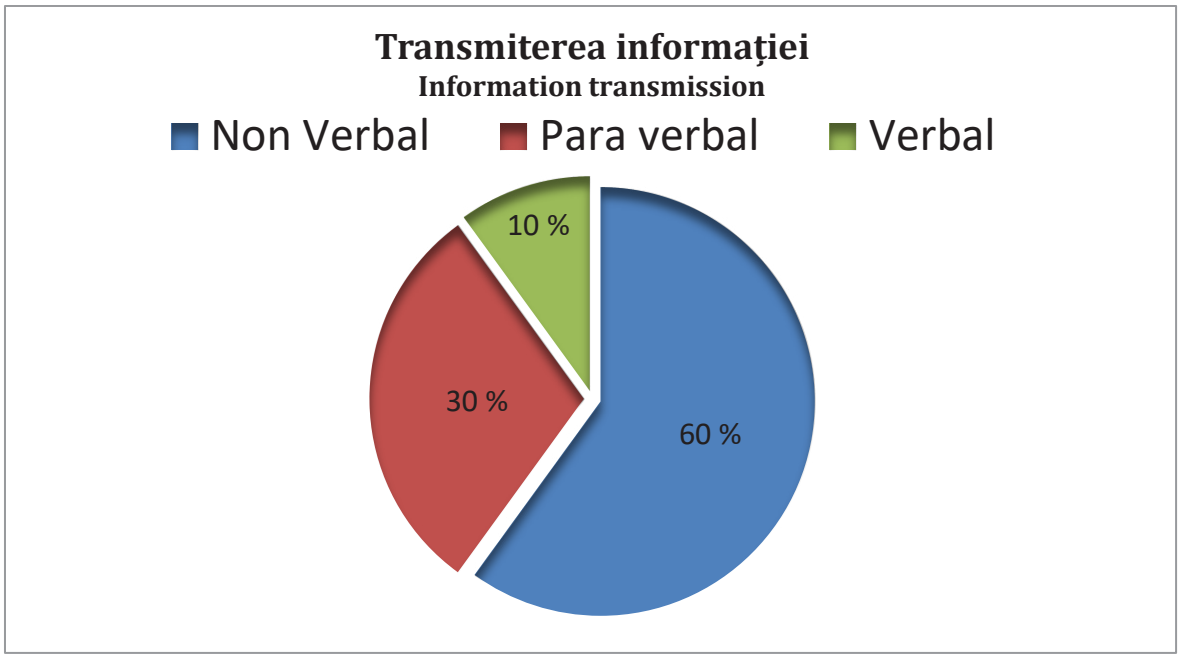
therefore give rise to physiological reactions that can be interpreted. Many physiological reactions that accompany simulated behavior are formed in the area of the autonomic nervous system and cannot be controlled by will.

Accordingly, an experienced profiler acts in the following way: he studies the behavior of a person in a situation where he is not required to lie. For example, have an abstract and relaxing discussion with the interviewee, followed by the stage when the stimuli are used. The stimuli are usually auditory, in the form of questions, but visual or sound stimuli can also be used.

We recommend that the interviewers be inspired by the tactical procedures used at the hearing, such as: the use of evidence of guilt or the tactic of surprise meetings [5].

Interviewers with experience in the activity of a criminal investigation officer, prosecutor, special investigation activity - people who, by virtue of their profession, have spent many specific activities similar to interviews, are considered extremely valuable.

During the interview, the non-verbal and para-verbal cues of the interviewee will be carefully analyzed. The weight of the transmission of information by a person is expressed in the following proportion:



Comunicarea nonverbală o însoţeşte pe cea verbală şi apare ca un element de întărire a acesteia.

Cel mai des întâlnite forme de comunicare nonverbală sunt:

- mimica (expresia facială),
- gestica,
- postura,
- atitudinea,
- vestimentaţia,
- comunicarea cu ajutorul distanţelor,
- comunicarea cu timpul.

Acestea confirmă sau infirmă mesajul verbal, în funcţie de manifestările lor.

Persoana care intenţionează să spună o minciună, trebuie să ascundă:

– Adevărul,

– Emoţia, ce apare odată cu comportamentul simulat.

Orice disimulare este fundamentată de un anume motiv, care are la bază frica de a fi pedepsit, dorinţa şi satisfacţia de a reuşi, sentimentul de vinovăţie, etc.

În acest context, disimularea este de obicei acoperită de gesturi, emoţii false neutre sau pozitive, care sunt considerate ca indicatori ai minciuni.

Lucrurile se complică în situaţiile în care persoanele sunt special pregătite pentru simularea comportamentului. Cea mai răspândită metodă este înlocuirea unui adevăr cu altul – tehnici ce îngreunează detecţia minciunii.

O selecţie calitativă a personalului, cu siguranţă va contribui la o creştere semnificativă a eficienţei întreprinderii.

Pentru rezolvarea problemelor cu personalul companiilor, în cadrul organizaţiilor sunt create structuri speciale cu funcţii ce vizează asigurarea securităţii interne sau aceste funcţii sunt realizate de agenţii specializate.

Există diverse metode de evaluare a competenţei candidaţilor, care permit o clasificare cât mai precisă a candidaţilor pentru un post într-o anumită companie. Identificarea tuturor riscurilor, alegerea metodologiei potrivite şi stabilirea corectă a cerinţelor pentru candidat este sarcina unui specialist în recrutare cu experienţă.

În unele situaţii, totuşi, se impune aplicarea cunoştinţelor speciale în procesul de recrutare. Ne referim la aplicarea poligrafului în

Non-verbal communication accompanies the verbal one and appears as an element to strengthen it.

The most common forms of non-verbal communication are:

- mimicry (facial expression),
- gestures,
- posture,
- attitude,
- clothing,
- communication using distances,
- communication in time.

These confirm or deny the verbal message, depending on their manifestations.

The person who intends to tell a lie must conceal:

- The truth,
- Emotion, which appears together with the simulated behavior.

Any concealment is based on a certain reason, which is also based on fear of being punished, the desire and satisfaction of succeeding, feeling of guilt, etc.

In this context, dissimulation is usually covered by gestures, fake neutral or positive emotions, which are considered as indicators of lying.

Things get complicated in situations where people are specially trained to simulate the behavior. The most widespread method is to replace one truth with another - techniques that make it difficult to detect a lie.

A qualitative selection of personnel will certainly contribute to a significant increase in the efficiency of the enterprise.

In order to solve problems with company personnel, special structures are created within organizations with functions aimed at ensuring internal security or these functions are performed by specialized agencies.

There are various methods of assessing the competence of candidates, which allow for the most accurate classification of candidates for a position in a particular company.

Identifying all the risks, choosing the right methodology and correctly setting the requirements for the candidate is the task of an experienced recruitment specialist.

In some situations, however, it is necessary to apply special knowledge in the recruitment process. We refer to the application of the

domeniul relaţiilor de muncă. Făcând o analiză statistică, deducem că testările poligraf sunt destul de răspândite în lume.

Angajatorul este interesat să obţină cât mai multe informaţii despre candidatul la o funcţie în cadrul întreprinderii, mai ales atunci când atribuţiile unui astfel de angajat presupun o responsabilitate sporită faţă de activele companiei, accesul la strategia de dezvoltare a întreprinderii, accesul la date privind informaţiile care pot constitui un secret comercial.

Testările la poligraf în aceste situaţii se efectuează la etapa de preselecţie în cadrul unui concurs de preselecţie, pentru ocuparea funcţiei vacante în întreprindere. Datorită acestei verificări, angajatorul primeşte informaţii valoroase şi veridice despre: candidatul la funcţie; scopul real al angajării; dacă poate încredinţa accesul la segmente importante ale activităţii companiei.

O situaţie deosebită este în cazul angajării personalului pentru deservirea infrastructurilor critice. Deşi abordările diferă, având drept punct de plecare elementele comune cu privire la importanţa funcţionării în siguranţă şi efectele induse, conceptul de „infrastructură critică" poate fi asimilat cu orice entitate economică funcţională, care oferă produse, bunuri şi servicii de utilitate publică, vitale pentru întreaga societate şi a cărei distrugere, degradare ori aducere într-o stare nefuncţională produce un impact major în plan economico-social, la nivel micro- şi macro-regional [6].

Potrivit unei definiţii europene, la care ne alăturăm, la infrastructurile critice se referă: „instalaţii, reţele, servicii şi active care, în caz de oprire sau de distrugere, pot să producă efecte nocive asupra sănătăţii, securităţii sau bunăstării economice a cetăţenilor sau activităţilor guvernelor statelor UE".

Ameninţările şi pericolul major în aceste situaţii pot fi provocate de acţiuni teroriste, acte de sabotaj, etc. Complexitatea şi interdependenţa acestor infrastructuri impun măsuri speciale de protecţie atât la nivel naţional, cât şi la nivel internaţional.

Ne referim la sistemele de infrastructuri critice pentru care sunt stabilite măsuri speciale de protecţie, în cadrul Uniunii Europene [7], şi anume:

– Instalaţiile şi reţelele de distribuţie din

polygraph in the field of labor relations. By doing a statistical analysis, we deduce that polygraph tests are quite widespread in the world.

The employer is interested in obtaining as much information as possible about the candidate for a position in the company, especially when the duties of such an employee involve increased responsibility for the company's assets, access to the company's development strategy, access to information data, which may constitute a trade secret.

The polygraph tests in these situations are carried out at the pre-selection stage within a pre-selection competition, for filling the vacant position in the company. Thanks to this verification, the employer receives valuable and truthful information about the candidate for the position, the real purpose of the employment, and whether he can entrust access to important segments of the company's activity.

A special situation is in the case of hiring staff to service critical infrastructures.

Although the approaches differ, having as a starting point the common elements regarding the importance of safe operation and the induced effects, the concept of "critical infrastructure" can be assimilated to any functional economic entity, which offers products, goods and services of public utility, vital for the whole society and whose destruction, degradation or bringing into non-functioning state produces a major economic-social impact, at the regional micro and macro level [6].

According to a European definition, which we adhere to, critical infrastructure refers to: "facilities, networks, services and assets that, in case of shutdown or destruction, can produce harmful effects on the health, security or economic well-being of citizens or activities governments of the EU states".

The major threats and danger in these situations can be caused by terrorist actions, acts of sabotage, etc.

The complexity and interdependence of these infrastructures require special protection measures at the national and international level.

We refer to the critical infrastructure systems for which special protection measures are established within the European Union [7], and namely:

– Installations and distribution net-

domeniul energetic (sub-sectoare legate de energie electrică, petrol, gaze);

– Tehnologiile de comunicaţii şi informaţii;

– Instituţiile care asigură sectorul financiar-bancar şi pieţele de valori şi investiţii;

– Platformele şi instituţiile sistemului de sănătate;

– Mijloacele de producţie şi distribuţie pentru sectorul alimentar;

– Aprovizionarea cu apă;

– Transportul feroviar, rutier, aerian, pe apă şi instalaţiile aferente utilizate;

– Producţia, stocajul şi transportul produselor periculoase (materiale chimice, biologice, radiologice şi nucleare);

– Administraţia (armata, jandarmeria şi poliţia).

Factorul uman este un element indispensabil al activităţii în siguranţă a infrastructurilor critice, dar, în acelaşi timp, el este un element ce urmează să fie obiectul unei analize de risc bazate pe vulnerabilitatea acestuia şi impactul potenţial.

Directiva 2008/114/CE a Consiliului Europei din 8 decembrie 2008, privind identificarea şi desemnarea infrastructurilor critice europene şi evaluarea necesităţii de îmbunătăţire a protecţiei acestora, menţionează acest lucru în mod expres [8].

Tot mai des sunt solicitate examinările pentru stabilirea viciilor angajaţilor sau ale persoanelor ce urmează să fie angajate la serviciu. Ne referim la aşa vicii ca: dependenţa de droguri, dependenţa de consumul excesiv al băuturilor alcoolice, cleptomania etc.

Un rol aparte îl au examinările poligraf destinate stabilirii tuturor circumstanţelor ce ţin de anchetele de serviciu în cadrul companiilor. În orice colectiv sunt posibile furturi în proporţii mici, deteriorări intenţionate ale bunurilor, forme de intimidări şi agresiuni – situaţii cu care, de obicei, nu se adresează imediat la organele de poliţie. Serviciile de securitate încercă să lămurească lucrurile la nivelul său, iniţiind anchete de serviciu.

Un exemplu elocvent este o situaţie din propria practică ce se referea la un furt din geantă, care se afla într-un birou unde accesul era permis doar persoanelor care se cunoşteau de mult timp şi erau în relaţii foarte bune. În

works in the energy field; (under sectors related to electricity, oil, gas.)

– Communication and information technologies;

– The institutions that ensure the financial-banking sector and the stock and investment markets;

– Health system platforms and institutions;

– The means of production and distribution for the food sector;

– Water supply;

– Rail, road, air, water transport and related facilities used;

– Production, storage and transport of dangerous products (chemical, biological, radiological and nuclear materials);

– Administration (army, gendarmerie and police).

The human factor is an indispensable element of the safe operation of critical infrastructures, but at the same time, it is an element to be subject to a risk analysis based on its vulnerability and potential impact.

Directive 2008/114/EC of the Council of Europe of December 8, 2008, regarding the identification and designation of European critical infrastructures and the assessment of the need to improve their protection expressly mentions this [8].

More and more often, examinations are requested to establish the vices of employees or people to be employed at work. We refer to such vices as: drug addiction, addiction to excessive consumption of alcoholic beverages, kleptomania, etc.

A special role is played by polygraph examinations designed to establish all the circumstances within the framework of service investigations within companies. Small-scale thefts, intentional damage to property, forms of intimidation and aggression are possible in any group - situations that are usually not immediately addressed to the police. The security services are trying to clear things up at his level by initiating official inquiries.

An eloquent example is a situation from my own practice that referred to a theft from a bag, which was in an office where access was allowed only to people who had known each other for a long time and were on very good terms. In

această situaţie s-a dorit aflarea adevărului cu privire la dispariţia banilor din geantă, dar nu prin intermediul organelor poliţieneşti. Prin urmare a fost dispusă o anchetă de serviciu pentru stabilirea circumstanţelor dispariţiei banilor şi a fost solicitată petrecerea testării cu aplicarea poligrafului.

Dacă în exemplul de mai sus are de suferit doar reputaţia unei persoane din colectiv, în alte cazuri acţiunile angajaţilor vor supune riscurilor de reputaţie compania, care într-un final, implicit vor contribui la pierderi de ordin financiar.

Un studiu aprofundat cu privire la factorii ce ar putea declanşa apariţia riscurilor ce ţin de reputaţie îi aparţine domnului Manea Ciprian în cadrul tezei „Managementul riscului reputaţional în domeniul bancar", în care expres sunt puse în evidenţă etica şi integritatea factorului uman [9].

La ora actuală, există diferite categorii de documente şi politici ale corporaţiilor mari, ce reglementează riscurile de pierdere a reputaţiei.

Spre exemplu, o referire clară asupra factorilor ce pot provoca riscuri de reputaţie întâlnim în Politicile privind administrarea riscurilor semnificative în BC „Moldindconbank" S.A., ca fiind piloni de bază în orientarea activităţilor Băncii pe coordonate de eficienţă. [10].

În acest context, se menţionează: riscul de reputaţie operaţională, când o activitate, acţiune sau poziţie a băncii, a administratorilor şi/sau a persoanelor afiliate băncii va dăuna imaginii băncii, astfel încât va fi afectat profitul fondurilor proprii ale băncii [10, p.5].

Vom aduce un exemplu din propria practică: „La o bancă comercială din Republica Moldova, în cadrul serviciului de securitate au apărut suspiciuni cu privire la o persoană cu dreptul de decizie, precum că ar favoriza acordarea de credite persoanelor, încălcând procedurile impuse în acest sens. A fost luată decizia aplicării poligrafului pentru a stabili circumstanţele acestui fapt. Urmare a acestei măsuri, au fost înlăturaţi factorii ce aduceau băncii prejudicii de ordin material şi de reputaţie.

Datorită faptului că poligraful a reuşit să rezolve o situaţie complicată în termeni restrânşi, cu păstrarea unui grad de confidenţialitate, banca a luat decizia să modi-

this situation, they wanted to find out the truth about the disappearance of the money from the bag, but not through the police. Therefore, a service investigation was ordered to establish the circumstances of the disappearance of the money and a polygraph test was requested.

If in the above example only the reputation of one person from the collective suffers, in other cases the actions of the employees will subject the company to reputational risks which in the end, implicitly, will also contribute to financial losses.

An in-depth study on the factors that could trigger the appearance of reputational risks belongs to Mr. Manea Ciprian in the thesis "Reputational risk management in the banking field", in which the ethics and integrity of the human factor are expressly highlighted [9].

Currently, there are different categories of documents and policies of large corporations, which regulate reputational risks.

For example, a clear reference to the factors that can cause reputational risks are provided in the Policies regarding the management of significant risks in BC "Moldindconbank" S.A., as basic pillars in orienting the Bank's activities on efficiency coordinates. [10].

Within this context, it has been mentioned: operational reputation risk, when an activity, action or position of the bank, administrators and/or persons affiliated with the bank will damage the bank's image, so that the bank's profit and own funds will be affected. [10, p. 5]

We will give an example from our own practice: "At a commercial bank in the Republic of Moldova, within the security service, suspicions arose regarding a person with the right to make decisions, as if he would favor the granting of loans to individuals, violating the procedures imposed in this sense. It was decided to apply the polygraph to establish the circumstances of this fact. Following this measure, the factors causing reputational and material damage to the bank were removed.

Due to the fact that the polygraph was able to solve a complicated situation in limited terms, while maintaining a degree of confidentiality, the bank made the decision to amend the individual employment contracts, introducing a clause whereby employees give their consent to be tested with the application of the poly-

fice contractele individuale de muncă, introducând o clauză prin care angajaţii dau acordul să fie testaţi cu aplicarea poligrafului cu o anumită periodicitate. În consecinţă, urmare a modificării contractelor de muncă, au depus cerere de eliberare din funcţia ocupată încă 4 şefi de filiale-factori de decizie în eliberarea creditelor.

Situaţia creată permite să concluzionăm, că poligraful a funcţionat şi ca măsură de profilaxie şi probabil ca măsură de prevenire. Însăţi condiţia în contract de a accepta testarea cu aplicarea poligrafului va contribui la micşorarea numărului candidaţilor cu intenţii şi scopuri „neloiale" companiei la care urmează să se angajeze.

Preocuparea principală a oricărui recrutor este înţelegerea atitudinii reale a unui candidat pentru ocuparea funcţiei la care urmează să fie angajat. Un recrutor are sarcina dificilă de a analiza un număr de persoane necunoscute şi de a identifica dintre acestea persoana cea mai potrivită pentru a ocupa postul vacant al companiei. La etapa interviului el are la dispoziţie doar CV-ul persoanei, fapt care îi permite să se informeze doar despre starea familială, studii, limbi vorbite etc., dar acest lucru nu este suficient.

O persoană care vrea cu orice preţ să obţină jobul, ar putea întocmi un CV cu date eronate, ascunzându-şi propriile defecte. De aici apar următoarele întrebări: cum se va prezenta persoana după angajare, cum va colabora cu colegii, cum va proceda în situaţii critice, cum va soluţiona conflictele cu clienţii, care sunt calităţile ei morale şi etice adevărate?

Angajaţii subdiviziunilor de securitate din cadrul companiilor au obligaţia să nu se limiteze doar la o analiză comportamentală a angajatului la etapa preselecţiei, ci să efectueze o analiză amplă a acestora şi pe perioada ulterioară.

Natura umană în permanenţă se află într-un proces de schimbare şi modificare în funcţie de anumiţi factori. În acest sens, omul suferă modificări comportamentale sub influenţa mediului în care se află. Iar locul de muncă este un mediu ce poate schimba comportamentul persoanei spre bine sau spre rău şi, din acest motiv, angajatul urmează să fie în continuare „tutelat".

Procedura de analiză comportamentală a angajatului poate fi împărţită în câteva acţiuni manageriale:

✓ Analiza pe perioada de adaptare;

graph with a certain periodicity. Consequently, as a result of the change in the employment contracts, 4 more heads of branches-decision-makers in the granting of loans submitted a request to be released from their position.

The situation created allows us to **conclude** that the polygraph also worked as a prophylactic measure and probably as a preventive measure. The condition in the contract to accept polygraph testing will contribute to reducing the number of candidates with intentions and goals "disloyal" to the company they are going to work for.

The main concern of any recruiter is to understand the real attitude of a candidate for the position to be hired.

A recruiter has the difficult task of sifting through a number of unknown people and identifying among them the most suitable person to fill the company's vacancy. At the interview stage, he only has the person's CV at his disposal, which allows him to find out information only about family status, studies, languages spoken, etc., but this is not enough.

A person who, wants by all means, to get the job could draw up a CV with erroneous data, hiding their own flaws. In consequence, questions arise related to how the person will present himself after employment: how will he collaborate with colleagues, how will he proceed in critical situations, how will he resolve conflicts with clients, what are the true moral and ethical qualities?

The employees of the security subdivisions within the companies are obliged not only to conduct a behavioral analysis of the employee at the pre-selection stage, but also to conduct an extensive analysis of them in the subsequent period as well.

Human nature is constantly in a process of change, modification according to certain factors. In this sense, he undergoes behavioral changes under the influence of the environment in which he is. The workplace is an environment that can change the person's behavior for better or worse and for this reason, the employee should continue to be "guarded".

The employee behavioral analysis procedure can be divided into several managerial actions:

✓ Analysis during the adaptation period;

✓ Prin acceptarea sau respectarea de către angajat a normelor comportamentale impuse de regulamentele interne;

✓ Atestarea angajatului.

O importanţă deosebită trebuie acordată unei analize a activităţii candidatului la locul precedent de lucru. Este des întâlnită practica concedierii angajatului şi, odată cu aceasta, el pleacă cu baza de clienţi sau sustrage toate materialele din calculatorul de serviciu. Orice angajator trebuie să fie atent cu asemenea persoane, care în mod sigur vor proceda în acelaşi mod şi în raport cu alte companii ce urmează să le angajeze.

Generalizând cele expuse, conchidem că „recruiting"-ul este asociat în mod constant cu riscuri – atât la etapa de preselecţie a candidatului, cât şi pe perioada de probă, activitate propriu-zisă şi concediere.

Pentru a menţine o reputaţie bună şi un climat favorabil pe interior, companiile ar trebui să atragă mai multă atenţie angajaţilor săi şi să nu ignore recomandările cu privire la procedurile ce vizează o serie de verificări, începând cu locul de muncă anterior, precum şi verificări speciale necesare ocupării postului de muncă (psihologice, medicale etc.).

Considerăm că un factor extrem de important, care trebuie avut în vedere, este loialitatea angajatului. Verificarea loialităţii este posibilă prin aplicarea cunoştinţelor speciale pentru detectarea comportamentului simulat prin aplicarea poligrafului. Acurateţea sistemelor computerizate contemporane se apropie de 98%, lucru ce permite detectarea intenţiilor ascunse ale angajatului.

În situaţiile aplicării poligrafului pentru testarea angajaţilor, recomandăm folosirea testelor construite după metodologia „Întrebările de control".

De remarcat că angajaţii loiali păzesc cu stricteţe secretele comerciale ale companiei. Sunt mereu în gardă, controlează posibilele ameninţări şi le contracarează. În mod cert, un angajat loial nu va trăda în niciun caz interesele companiei.

✓ Through the employee's acceptance and compliance with the behavioral norms imposed by the internal regulations;

✓ Attestation of the employee;

Particular importance should be given to an analysis of the candidate's activity at the previous workplace. It is common practice to fire the employee and with him he leaves with the customer base or all the materials from the work computer. Any employer must be careful with such people, he will do exactly the same in relation to other companies that are going to hire him.

Generalizing the above, we conclude that recruiting is constantly associated with risks - both at the candidate pre-selection stage, as well as during the trial period, actual activity and dismissal.

In order to maintain a good reputation and a favorable internal climate, interested companies should pay more attention to their employees and should not ignore the recommendations regarding the procedures aimed at a series of checks, starting with the previous workplace, as well as checks special requirements for employment (psychological, medical, etc.).

We consider an extremely important factor that must be taken into account - the loyalty of the employee. Loyalty verification is possible through the application of special knowledge in the detection of simulated behavior through the application of the polygraph. The accuracy of contemporary computerized systems approaches 98%, which allows the detection of the hidden intentions of the employee.

In the situations of applying the polygraph for testing employees, we recommend using tests built according to the "Control questions" methodology.

Loyal employees strictly guard the company's trade secrets. They are always on guard, control possible threats and counter them. For a loyal employee, betraying the interests of the company is simply impossible.

Referinţe bibliografice

Bibliographical references

1. Benjamin C. Glassman, Matt Wagner, Colin R. Jennings. Economic Espionage and Theft of Trade Secrets. National Law Review, Volume XII, Number 55, February 24, 2022.
2. Bailouts and the Potential for Distortion of Federal Criminal Law: Industrial Espionage and Beyond, 86 TULANE LAW REVIEW 1017 (2012).
3. „United States v. Williams" Oyez, www.oyez.org/cases/2007/06-694. Accesat 27 Dec. 2022.
4. Шлыков В.В. Комплексное обеспечение экономической безопасности предприятия. Издательство «Алетея», 1999.
5. Tudor Osoianu, Iurie Odagiu, Dinu Ostavciuc, Constantin Rusnac, „Tactica acţiunilor de urmărire penală", editura Cartea Militară, 2020.
6. International Journal of Critical Infrastructures, vol. 1, nr.1/2004.
7. Communication from the Commission of 12 December 2006 on a European Programme for Critical Infrastructure Protection [COM(2006) 786 final – Official Journal C 126 of 7.6.2007].
8. https://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?ri=CELEX:32008L0114&from=CS, vizitat 04.01.2023.
9. Rezumatul tezei de doctorat (în limbile română şi engleză) poate fi consultat în cadrul Depozitului digital instituţional ARTHRA la adresa: http://www.arthra.ugal.ro; Teza de doctorat în format tipărit poate fi consultată la biblioteca universităţii „Dunărea de Jos" din Galaţi.
10. https://www.micb.md/img/n-info-doc/Administrare_riscuri_2021.pdf, vizitat 04.01.2023.

Despre autori:

Iurie ODAGIU,
doctor în drept, conferenţiar universitar,
prim-prorector pentru studii
şi management al calităţii,
Academia „Ştefan cel Mare" a MAI,
e-mail: criminalistic@gmail.com,
ORCID: 0000-0002-2474-5299

Andrei LUNGU,
doctorand,
Şcoala doctorală „Ştiinţe penale şi drept public",
Academia „Ştefan cel Mare" a MAI,
master în drept,master în psihologie,
poligrafolog
e-mail: andrei.lungu@mai.gov.md
ORCID: 0000-0003-0214-828X

About authors:

Iurie ODAGIU,
PhD, associate professor,
First Vice-Rector for studies
and quality management of the
Academy "Stefan cel Mare"of the MIA,
e-mail: criminalistic@gmail.com,
ORCID: 0000-0002-2474-5299

Andrei LUNGU,
PhD student,
Doctoral School "Criminal Sciences and Public Law",
Academia „Ştefan cel Mare" a MAI,
master in law, master in psychology,
polygraph examiner,
e-mail: andrei.lungu@mai.gov.md
ORCID: 0000-0003-0214-828X